ELSEVIER

Discrete Applied Mathematics 114 (2001) 95–108

DISCRETE APPLIED MATHEMATICS

On an infinite sequence of improving Boolean bases ☆

D.U. Cherukhin

Moscow State University, Moscow, 119899 Russia

Abstract

We consider complexity of formulas for Boolean functions in finite complete bases. It is shown that, as regards complexity, the basis of all $(k+1)$-ary functions is essentially better than the basis of all k-ary functions for all $k \geqslant 2$. © 2001 Published by Elsevier Science B.V.

Keywords: Boolean function; Formula; Complexity

There are two approaches in comparing classes of control systems: global, with regard to complexity of formulas for almost all functions, and local, regarding the complexity of formulas for individual sequences of functions. As shown by Lupanov [1], with global approach all finite bases are equivalent, their Shannon functions have the same order. Meanwhile, Subbotovskaya [4] has established that in the basis $\{\&, \vee, \neg\}$ the complexity of linear Boolean functions of n arguments is higher than in the basis $\{\&, \oplus, 1\}$. Thus, the local approach in comparing bases is of certain interest; and it will be studied in the present paper.

We shall need some definitions. The *complexity of a formula* F, denoted by $L(F)$, is the number of occurrences of variables. The *complexity of a Boolean function* f in a basis B, $L_B(f)$ is the minimal complexity of formulas computing the function f. The basis B_1 is said to be *not worse* than the basis B_2, $B_1 \preccurlyeq B_2$, if there exists a positive constant C such that $L_{B_1}(f) \leqslant C L_{B_2}(f)$ for any Boolean function f. Bases B_1 and B_2 are said to be *equivalent*, $B_1 \sim B_2$, if $B_1 \preccurlyeq B_2$ and $B_2 \preccurlyeq B_1$. The basis B_1 is said to be *better* than the basis B_2, $B_1 \prec B_2$, if $B_1 \preccurlyeq B_2$, while $B_2 \preccurlyeq B_1$ is not true.

It was shown by Lupanov [1] that any basis is not worse than $B_0 = \{\&, \vee, \neg\}$. Subbotovskaya [4] established a criterion of equivalence to the basis B_0, and showed the existence of inequivalent bases; more exactly, she proved that the basis $B_1 = \{\&, \oplus, 1\}$ is better than the basis B_0. Stetsenko [3] described the close neighborhood of the basis B_0, i.e., the set of almost bad bases. As shown by Muchnik [2], each nonlinear basis

☆ Translated from *Discrete Anal. Oper. Res.* (Novosibirsk) 4(4) (1997) 79–95. This research was supported by the Russian Foundation of Basic Research (Grant 96-01-01068).

0166-218X/01/$ - see front matter © 2001 Published by Elsevier Science B.V.
PII: S0166-218X(00)00362-0

B is inequivalent to the basis B_1 and $B \cup B_1 \prec B$. Thus, if B is a nonlinear basis not equivalent to B_0 then bases $B \cup B_1$, B and B_0 generate a sequence of length 3 ordered by relation $\prec$, i.e., $B \cup B_1 \prec B \prec B_0$.

In the present paper we establish that the bases $\{P_2(n) \mid n \geqslant 2\}$ consisting of all n-ary Boolean functions generate an infinite sequence ordered by relation $\prec$, i.e., $P_2(n+1) \prec P_2(n)$ for each $n \geqslant 2$. In order to prove the main theorem, the system of functions $\{f_n^{(m_k)} \mid n \in N,\ k \in N\}$ will be presented such that for each $n \geqslant 2$

$$\frac{L_{P_2(n)}(f_{n+1}^{(m_k)})}{L_{P_2(n+1)}(f_{n+1}^{(m_k)})} \to \infty \quad \text{for } k \to \infty.$$

Let F be an arbitrary formula in the basis B. Define by induction the *subformulas* of the formula F:

(1) if $F \equiv x_i$, then the only subformula of the formula F is F;
(2) if $F \equiv f(G_1, \ldots, G_s)$ and $f \in B$, then F and all subformulas of formulas $G_1, \ldots, G_s$ are also subformulas of the formula F. In this case, the formulas $G_1, \ldots, G_s$ will be called *immediate subformulas* of the formula F.

In what follows, the formula $\Lambda_n^c(G_1, \ldots, G_n)$, where Λ_n is the linear function of n arguments having value c on the null set, will be denoted by $G_1 \oplus \cdots \oplus G_n \oplus c$. Let us call the formula $F' \equiv F_1 \oplus F_2 \oplus c$ the *linear representation* of the formula F if F' computes the same function as F, $L(F') \leqslant L(F)$, and none of the formulas F_1, F_2 is a constant.

Let F be an arbitrary formula in the basis $P_2(n)$. We shall perform the following transformations of the formula F:

(1) Each subformula of F having a linear representation and not being the linear representation of itself will be replaced with its linear representation.
(2) Each subformula of the formula F which computes the linear function $x_{i_1} \oplus \cdots \oplus x_{i_s} \oplus c$ but has a subformula computing a nonlinear function, will be replaced with the subformula $(\ldots(x_{i_1} \oplus x_{i_2}) \oplus \ldots) \oplus x_{i_s} \oplus c$;
(3) Each subformula of the formula F having the form $f(G_1, \ldots, G_i, c, G_{i+1}, \ldots, G_s)$ will be replaced with the subformula $g(G_1, \ldots, G_s)$, where c is a constant and $g(x_1, \ldots, x_s) \equiv f(x_1, \ldots, x_i, c, x_{i+1}, \ldots, x_s)$.

Finally, we obtain the formula F' with the following properties:

(r1) F' is a formula in the basis $P_2(n)$;
(r2) F' computes the same function as F, and $L(F') \leqslant L(F)$;
(r3) each subformula G of the formula F' has one of the two forms:
  (i) $G \equiv f(G_1, \ldots, G_s)$, where $2 \leqslant s \leqslant n$, G has no linear representation and all formulas G_i are not constant;
  (ii) $G \equiv G_1 \oplus \cdots \oplus G_s \oplus c$;
(r4) none of the subformulas of the formula F' which compute a linear function has a subformula computing a nonlinear function.

We call the formula F' with properties (r1)–(r4) the *reduced* formula for F. Unless otherwise stated, we shall consider all formulas as being reduced.

Let G be an arbitrary formula of the form (i). The immediate subformula of the formula G will be called *chosen* if all other immediate subformulas of the formula G compute linear functions. We shall call the formula G a *μ-formula* if at least one of its immediate subformulas is chosen. The formula G will be called a *center* if all immediate subformulas of G compute linear functions; each center is a μ-formula. The *constants substitution* will mean a mapping from a certain finite subset of variables into the set $\{0,1\}$.

We introduce the following notation:

- $n(F)$ is the number of different variables in the formula F;
- $m(F)$ is the greatest number of occurrences of one variable in F;
- $nes(f)$ is the number of essential variables of the function f;
- $L_n(f)$ is the complexity of the function f in the basis $P_2(n)$;
- $\{\tilde{x}=\tilde{c}\}$ or $\{x_{i_1}=c_{i_1},\ldots,x_{i_k}=c_{i_k}\}$ is the constants substitution which brings each variable x_{i_j} of $\tilde{x}=(x_{i_1},\ldots,x_{i_k})$ in correspondence with the constant c_{i_j} of $\tilde{c}=(c_{i_1},\ldots,c_{i_k})$;
- $|A|$ is the size of the constants substitution A, i.e., the number of variables brought in correspondence with constants;
- $F|_A$ is the formula obtained from the formula F by replacing all symbols of variables defined in the constants substitution A with corresponding constants and subsequent reduction;
- $f|_A$ is the function obtained from the function f by the substitution of variables defined in the constants substitution A with corresponding constants; the function $f|_A$ will be called the *subfunction* of f;
- $\mu(F)$ is the number of subformulas of the formula F which are μ-formulas, or the number of μ-subformulas of F;
- $z(F)$ is the number of centers among subformulas of the formula F, or the number of centers of F;
- $d(f)$ is the degree of Zhegalkin polynomial of the function f; if $f\equiv 1$ or $f\equiv 0$, then $d(f)=0$.

We recall some properties of the degree. Let $g\in P_2(s)$, $g_1,\ldots,g_s$ be arbitrary functions, and c an arbitrary constant. Then

(d1) $d(g(g_1,\ldots,g_s))\leqslant\sum_{i=1}^{s} d(g_i)$;

(d2) $d(g_1\oplus\cdots\oplus g_s\oplus c)\leqslant\max_{1\leqslant i\leqslant s} d(g_i)$;

(d3) if $d(g)=s$ and $g_1,\ldots,g_s$ essentially depend on non-empty and mutually disjoint sets of variables, then $d(g(g_1,\ldots,g_s))=\sum_{i=1}^{s} d(g_i)$.

Lemma 1. *If F is a formula in the basis $P_2(n)$ computing an arbitrary nonlinear function f, then*

$$\mu(F)\geqslant\frac{1}{2n}d(f)+\frac{1}{2}.$$

Proof. We use the induction on constructing the formula F. Basis of induction: all immediate subformulas of the formula F compute linear functions, whereas F, a nonlinear

one. Then F is a center. From (d1) it follows that $d(f)\leqslant n$. Therefore,

$$\mu(F)=1=\frac{1}{2n}n+\frac{1}{2}\geqslant\frac{1}{2n}d(f)+\frac{1}{2}.$$

Induction step: let at least one of the immediate subformulas of the formula F compute a nonlinear function.

Let $G_1,\dots,G_s$ be the immediate subformulas of the formula F and G_i compute the function g_i; let the functions $g_1,\dots,g_k$ be nonlinear, $k\geqslant 1$, let $g_{k+1},\dots,g_s$ linear. By the induction hypothesis, for any i, $1\leqslant i\leqslant k$, we have

$$\mu(G_i)\geqslant\frac{1}{2n}d(g_i)+\frac{1}{2}.$$

Two cases are possible: (1) F has the form (i); (2) F has the form (ii).

Case 1. Let $F\equiv g(G_1,\dots,G_s)$. Then $f=g(g_1,\dots,g_s)$. Therefore, property (d1) and the inequality $s\leqslant n$ imply that

$$d(f)\leqslant\sum_{i=1}^{s}d(g_i)=\sum_{i=1}^{k}d(g_i)+(s-k)\leqslant\sum_{i=1}^{k}d(g_i)+n.$$

If $k=1$, then F is a μ-formula. Therefore,

$$\mu(F)=\mu(G_1)+1\geqslant\frac{1}{2n}d(g_1)+\frac{1}{2}+1\geqslant\frac{1}{2n}d(g_1)+1.$$

But if $k\geqslant 2$, then F is not a μ-formula and

$$\mu(F)=\sum_{i=1}^{k}\mu(G_i)\geqslant\frac{1}{2n}\sum_{i=1}^{k}d(g_i)+\frac{k}{2}\geqslant\frac{1}{2n}\sum_{i=1}^{k}d(g_i)+1.$$

Thus, for any k we have

$$\mu(F)\geqslant\frac{1}{2n}\sum_{i=1}^{k}d(g_i)+1=\frac{1}{2n}\left(\sum_{i=1}^{k}d(g_i)+n\right)+\frac{1}{2}\geqslant\frac{1}{2n}d(f)+\frac{1}{2}.$$

Case 2. Let $F\equiv G_1\oplus\cdots\oplus G_s\oplus c$. Using (d2) we obtain

$$\begin{aligned}\mu(F)&=\sum_{i=1}^{k}\mu(G_i)\geqslant\frac{1}{2n}\sum_{i=1}^{k}d(g_i)+\frac{k}{2}\geqslant\frac{1}{2n}\max_{1\leqslant i\leqslant k}d(g_i)+\frac{1}{2}\\&=\frac{1}{2n}\max_{1\leqslant i\leqslant s}d(g_i)+\frac{1}{2}\geqslant\frac{1}{2n}d(f)+\frac{1}{2}.\qquad\square\end{aligned}$$

Let F be a formula, and let $\mu_1,\dots,\mu_t$ be a sequence of different μ-formulas, μ_i being a subformula of the formula μ_{i+1} for $1\leqslant i\leqslant t-1$ and μ_t a subformula of the formula F. Then the sequence $\mu_1,\dots,\mu_t$ will be called the *μ-chain* of the formula F. The μ-chain of the formula F to which no other μ-subformula of the formula F can be added will be called the *maximal μ-chain* of the formula F.

Lemma 2. *Suppose that some μ-subformulas of the formula F are marked in some manner, the number of marked formulas is equal to Q, and each μ-chain of the formula F has at most T marked formulas. Then*

$$T \cdot z(F) \geqslant Q.$$

Proof. We establish a one-to-one correspondence between all maximal μ-chains of the formula F and all centers of the formula F. Let $\mu_1, \ldots, \mu_t$ be an arbitrary maximal μ-chain of the formula F. Let us show that μ_1 is a center. Indeed, otherwise μ_1 would have an immediate subformula computing a nonlinear function and this subformula would have an immediate subformula with some center μ_0. One can easily see that each formula computing a nonlinear function does have at least one center. Then the sequence $\mu_0, \mu_1, \ldots, \mu_t$ would be a μ-chain of the formula F, contrary to the condition of initial μ-chain being maximal. Let the μ-chain $\mu_1, \ldots, \mu_t$ be corresponding to the center μ_1. This correspondence is one-to-one since from each μ-formula $\mu_i, 1 \leqslant i \leqslant t-1$, the next μ-formula μ_{i+1} can be restored uniquely. Denoting by M the number of maximal μ-chains of the formula F, we obtain $z(F)=M$. Since each μ-subformula of the formula F is a μ-chain, it follows that it is contained in some maximal μ-chain of the formula F. By the statement of the lemma, each maximal μ-chain of the formula F has at most T marked formulas. Therefore, the total number of marked subformulas of the formula F does not exceed TM. Hence,

$$T \cdot z(F) = TM \geqslant Q. \qquad \square$$

We shall call the formula G *fillable* if G is a μ-formula and some chosen subformula of the formula G has a variable which other immediate subformulas of the formula G do not have.

Lemma 3. *If a formula F has a μ-chain of t nonfillable μ-formulas and $m(F) \geqslant 1$, then*

$$L(F) \geqslant \left(1 + \frac{1}{m(F)}\right)^t.$$

Proof. We use the induction on t. If $t = 1$ then F has a μ-chain of length 1, that is, a μ-subformula. Therefore, $L(F) \geqslant 2 \geqslant (1 + 1/m(F))$.

Suppose the lemma is valid for any $i \leqslant t-1$, $t \geqslant 2$. Let $\mu_1, \ldots, \mu_{t-1}, \mu_t$ be a μ-chain in F such that none of formulas μ_i is fillable. By the induction hypothesis, we have

$$L(\mu_{t-1}) \geqslant \left(1 + \frac{1}{m(F)}\right)^{t-1}.$$

Let $G_1, \ldots, G_s$ be immediate subformulas of the formula μ_t, and let, for definiteness, G_1 be chosen. The formulas $G_2, \ldots, G_s$ compute linear functions, while μ_{t-1} computes a nonlinear one. Therefore, from property (r4) of reduced formulas it follows that μ_{t-1} is a subformula of G_1, and so

$$L(G_1) \geqslant L(\mu_{t-1}).$$

Since the formula μ_t is nonfillable, each variable in G_1 is present in at least one of formulas $G_2, \ldots, G_s$. Hence,

$$\sum_{i=2}^{s} n(G_i) \geqslant n(G_1).$$

Note that $L(G_i) \geqslant n(G_i)$ for any i, $2 \leqslant i \leqslant s$, and $L(G_1) \leqslant m(F)n(G_1)$. It follows from these inequalities that

$$L(F) \geqslant L(\mu_t) = L(G_1) + \sum_{i=2}^{s} L(G_i) \geqslant L(G_1) + \sum_{i=2}^{s} n(G_i)$$
$$\geqslant L(G_1) + n(G_1) \geqslant L(G_1)\left(1 + \frac{1}{m(F)}\right) \geqslant \left(1 + \frac{1}{m(F)}\right)^t. \qquad \square$$

Let a function f be not constant, and $s = nes(f)$. We define a family of formulas $\{\langle f\rangle_i^{(m)} \mid i \in N,\ m \in N \cup \{0\}\}$ by induction. We set

$$\langle f\rangle_i^{(0)} \equiv x_i, \quad \langle f\rangle_i^{(m+1)} \equiv f(\langle f\rangle_i^{(m)}, \langle f\rangle_{i+s^m}^{(m)}, \ldots, \langle f\rangle_{i+s^m(s-1)}^{(m)}).$$

For different i formulas $\langle f\rangle_i^{(m)}$ are obtained one from another by a change of variables without identification. Hereinafter, $\langle f\rangle^{(m)}$ will denote any of them, and $f^{(m)}$ will denote the function computed by the formula $\langle f\rangle^{(m)}$.

Contrary to our previous agreements, in this context only, we consider formulas of the form $\langle f\rangle^{(m)}|_A$, where $A = \{\tilde{x} = \tilde{c}\}$, as being the result of substituting constants from $\tilde{c}$ for corresponding variables of $\tilde{x}$ in the formula $\langle f\rangle^{(m)}$, without any further transformations.

Let $g = f^{(m)}|_A$, $m \geqslant 1$. Functions computed by immediate subformulas of the formula $\langle f\rangle^{(m)}|_A$ will be called *immediate subfunctions* of the function g. Note that immediate subfunctions of the function g are subfunctions of the function $f^{(m-1)}$, and the sets of their variables are mutually disjoint.

Proposition 1. *Suppose* $m \geqslant 1$, $nes(f) = s$, *and some* $(s-1)^m + 1$ *variables of the function* $f^{(m)}$ *are marked in some manner. Then there exists a subformula of the formula* $\langle f\rangle^{(m)}$ *such that each of its immediate subformulas has a marked variable.*

Proof. We use the induction on m. If $m = 1$, then $(s-1)^m + 1 = s$, and we can take the formula $\langle f\rangle^{(1)}$ as the required formula.

Let $m \geqslant 2$. Two cases are possible:

(1) we can take the formula $\langle f\rangle^{(m)}$ as the required formula;

(2) $\langle f\rangle^{(m)}$ has an immediate subformula which does not have marked variables. Using the Dirichlet principle, one can easily see that $\langle f\rangle^{(m)}$ has another immediate subformula that has at least $\lceil (s-1)^m + 1/s - 1 \rceil = (s-1)^{m-1} + 1$ marked variables. It remains to apply the induction hypothesis to it. $\square$

Let the formula F compute a function g. Denote by $N(q,F)$ the number of essential variables of g which occur in F at most q times each.

Lemma 4. *Let g be a subfunction of the function $f^{(m)}$, $m \geqslant 1$, let F be a formula in the basis $P_2(n)$ which computes the function g, and let $L_n(f) > q\, nes(f)$ for some $q \geqslant 0$. Then*

$$N(q,F) \leqslant (nes(f)-1)^m.$$

Proof. Suppose the contrary, i.e., $N(q,F) > (nes(f)-1)^m$. Then $N(q,F) \geqslant (s-1)^m+1$, where $s = nes(f)$. Let $g = f^{(m)}|_A$. Let us mark the essential variables of the function g; these variables will be at the same time variables of the function $f^{(m)}$, each of them occurring in F not more than q times. According to Proposition 1, the formula $\langle f\rangle^{(m)}$ has a subformula $G \equiv f(G_1,\ldots,G_s)$ such that each subformula G_i has some marked variable x_{k_i}. Since the formula $\langle f\rangle^{(m)}|_A$ computes the function g, the formula $G_i|_A$ essentially depends on x_{k_i} for each i. Hence, there exist a constants substitution A_i and a constant σ_i such that $(G_i|_A)|_{A_i}$ computes the function $x_{k_i} \oplus \sigma_i$ and A_i is defined only on variables of G_i. Each variable occurs in $\langle f\rangle^{(m)}|_A$ at most once and the formula $\langle f\rangle^{(m)}|_A$ essentially, depends on the subformula $G|_A$. Therefore, there exist a constants substitution A_0 and a constant σ_0 such that the formula $(\langle f\rangle^{(m)}|_A)|_{A_0}$ computes the same function as the formula $G|_A \oplus \sigma_0$. We set $B = \bigcup_{i=0}^{s} A_i$. The formula $(\langle f\rangle^{(m)}|_A)|_B$ computes the function $g|_B = f(x_{k_1} \oplus \sigma_1,\ldots,x_{k_s} \oplus \sigma_s) \oplus \sigma_0$. Since the basis $P_2(n)$ contains negation, it follows that $L_n(g|_B) = L_n(f)$. Now the hypothesis of our lemma implies that $L_n(g|_B) > qs$. On the other hand, due to the choice of marked variables we have $L_n(g|_B) \leqslant L(F|_B) \leqslant qs$. A contradiction. □

Let g be a subfunction of the function $f^{(m)}$, $g = f^{(m)}|_A$. The essential variable x_i of the function g will be called *singular* if the formula $\langle f\rangle^{(m)}|_A$ has a subformula which contains x_i, and has an immediate subformula which computes a constant. The number of singular variables of the function g will be denoted by $I(g)$.

Lemma 5. *Suppose that g is an arbitrary subfunction of the function $f^{(m)}$. Then*
(a) $I(g) \leqslant (nes(f)-1)(nes(f^{(m)}) - nes(g))$;
(b) *if* $d(f) = nes(f)$, *then* $d(g) \geqslant nes(g) - I(g)$;
(c) *if* $I(g) = 0$ *and* $nes(g) > 0$, *then* $g = f^{(m)}$.

Proof. We use the induction on m; set $s = nes(f)$.

If $m = 0$, then g is either a variable or a constant. Therefore, $I(g) = 0$. Hence,
(a) $I(g) = 0 \leqslant (s-1)(1-nes(g)) = (s-1)(nes(f^{(0)}) - nes(g))$;
(b) $d(g) = nes(g) \geqslant nes(g) - I(g)$;
(c) $nes(g) > 0$ implies that $g = f^{(0)}$.

Let $m \geqslant 1$, and let $g_1,\ldots,g_s$ be immediate subfunctions of the function g. Two cases are possible: (1) there is a constant among g_i, i.e., a function identical to 0 or 1; (2) there is no constant among g_i.

Case 1. All essential variables of the function g are singular, i.e., $nes(g) = I(g)$. Therefore,

(a) $I(g) = nes(g) \leqslant (s-1)nes(f^{(m-1)}) = (s-1)s^{m-1} = (s-1)(s^m - (s-1)s^{m-1}) \leqslant (s-1)(s^m - nes(g))$;

(b) $d(g) \geqslant 0 = nes(g) - I(g)$;

(c) cannot happen.

Case 2. $nes(g) = \sum_{i=1}^{s} nes(g_i)$ and $I(g) = \sum_{i=1}^{s} I(g_i)$.

By the induction hypothesis, we have

(a) $I(g) = \sum_{i=1}^{s} I(g_i) \leqslant \sum_{i=1}^{s} (s-1)(s^{m-1} - nes(g_i)) = (s-1)(s^m - nes(g))$;

(b) from $d(f) = nes(f)$ and property (d3) it follows that $d(g) = \sum_{i=1}^{s} d(g_i) \geqslant \sum_{i=1}^{s} (nes(g_i) - I(g_i)) = nes(g) - I(g)$;

(c) from $I(g) = 0$ it follows that $I(g_i) = 0$ for each i; therefore, $g_i = f^{(m-1)}$. This means that $g = f(f^{(m-1)}, \ldots, f^{(m-1)}) = f^{(m)}$. □

For each $s \geqslant 1$ define

$$f_s(x_1, \ldots, x_s) = x_1 x_2 \ldots x_s \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_s.$$

Proposition 2. *Suppose that g is a subfunction of the function $f_s^{(m)}$, where $s \geqslant 2$ and $m \geqslant 1$, and $g_1, \ldots, g_s$ are immediate subfunctions of the function g of which at most $s-2$ are identical to one. Then*

$$nes(g) = \sum_{i=1}^{s} nes(g_i).$$

Proof. Let for definiteness $g_1, \ldots, g_k$ be identical neither to 0 nor to 1, and let $g_{k+1} \equiv \cdots \equiv g_n \equiv 0$, $g_{n+1} \equiv \cdots \equiv g_s \equiv 1$. Note that $f_i|_{\{x_i=1\}} = f_{i-1} \oplus 1$ and $f_i|_{\{x_i=0\}} = x_1 \oplus \cdots \oplus x_{i-1}$ for any $i \geqslant 2$. From the proposition statement it follows that $n \geqslant 2$. If $k = n$ then $g = f_s(g_1, \ldots, g_s) = f_k(g_1, \ldots, g_k) \oplus (s-n) \pmod 2$, and if $k < n$ then $g = g_1 \oplus \cdots \oplus g_k \oplus (s-n) \pmod 2$. Functions f_k for $k \geqslant 2$ and $x_1 \oplus \cdots \oplus x_k$ for any k essentially depend on all of their variables, and the sets of essential variables of functions g_i are mutually disjoint. Therefore,

$$nes(g) = \sum_{i=1}^{k} nes(g_i) = \sum_{i=1}^{s} nes(g_i). \qquad \square$$

Remark. The function f_s becomes a constant when $s-1$ ones are substituted into it.

Lemma 6. *Suppose that g is a subfunction of the function $f_s^{(m)}$, $s \geqslant 2$, and x_i is an essential variable of the function g. Then there exists a constant c such that*

$$nes(g) = nes(g|_{\{x_i=c\}}) + 1 \quad \textit{and} \quad g|_{\{x_i=c\}} \not\equiv 1.$$

Proof. We use the induction on m.

If $m = 0$, then it is sufficient to set $c = 0$.

Let $m \geqslant 1$. In the case $nes(g) = 1$ it suffices to choose a constant c such that $g(c) = 0$.

Consider the case $nes(g) > 1$. Let $g_1, \ldots, g_s$ be immediate subfunctions of the function g; assume for definiteness that x_i is a variable of the function g_1. From the Remark it follows that not all functions $g_2, \ldots, g_s$ are identical to one. By Proposition 2, we have

$$nes(g) = \sum_{i=1}^{s} nes(g_i). \tag{1}$$

By the induction hypothesis, for the function g_1 there exists a constant c such that

$$nes(g_1) = nes(g_1|_{\{x_i=c\}}) + 1 \quad \text{and} \quad g_1|_{\{x_i=c\}} \not\equiv 1. \tag{2}$$

Thus, among functions $g_1|_{\{x_i=c\}}, g_2, \ldots, g_s$ which are immediate subfunctions of the function $g|_{\{x_i=c\}}$ at most $s-2$ are identical to one. From this and by Proposition 2 it follows that

$$nes(g|_{\{x_i=c\}}) = nes(g_1|_{\{x_i=c\}}) + \sum_{i=2}^{s} nes(g_i). \tag{3}$$

From equalities (1)–(3), we obtain $nes(g) = nes(g|_{\{x_i=c\}}) + 1$. Then from $nes(g) > 1$ it follows that $nes(g|_{\{x_i=c\}}) > 0$, and this means that $g|_{\{x_i=c\}} \not\equiv 1$. □

Lemma 7. *Suppose that g is a subfunction of the function $f_s^{(m)}$, $s \geqslant 2$, and A is a constants substitution defined on some essential nonsingular variables of the function g. If among the constants substituted by A there are at most $s-2$ ones, then*

$$nes(g) = nes(g|_A) + |A|. \tag{4}$$

Proof. We use the induction on m.

If $m = 0$, then $nes(g) \leqslant 1$ and (4) is valid.

Let $m \geqslant 1$, and let $g_1, \ldots, g_s$ be immediate subfunctions of the function g. If at least one of the functions g_i is identical either to 0 or to 1, then all variables of the function g are singular, i.e., $A = \emptyset$ and (4) is valid.

Suppose $nes(g_i) > 0$ for each i. Then

$$nes(g) = \sum_{i=1}^{s} nes(g_i). \tag{5}$$

Let A_i be a restriction of the constants substitution A on the set of variables of the function g_i. Then

$$|A| = \sum_{i=1}^{s} |A_i|. \tag{6}$$

We can apply the induction hypothesis to the function g_i and obtain

$$nes(g_i) = nes(g_i|_{A_i}) + |A_i|. \tag{7}$$

Among constants substitutions A_i there are two, say, A_1 and A_2, which do not substitute the constant 1. Let A_j, $1 \leqslant j \leqslant 2$, be any of them. Let us show that $g_j|_{A_j} \not\equiv 1$. In the case

when $nes(g_j|_{A_j}) \geqslant 1$ it is plain. Let $nes(g_j|_{A_j}) = 0$. Then $nes(g_j) = |A_j|$; and it follows from Lemma 7 that all variables of the function g_j are nonsingular, i.e., $I(g_j) = 0$. Lemma 5(c) implies that $g_j = f_s^{(m-1)}$. Since the function f_s preserves zero, so does $f_s^{(m-1)}$, and this means that $g_j|_{A_j} \equiv 0 \neq 1$. Thus, among the functions $g_i|_{A_i}$, $1 \leqslant i \leqslant s$, at most $s-2$ are identical to zero. By Proposition 2, it follows that

$$nes(g|_A) = \sum_{i=1}^{s} nes(g_i|_{A_i}). \tag{8}$$

From (5)–(8) we have (4). □

Theorem 1. *For any natural $n \geqslant 2$ there exists a sequence of natural numbers (m_k) such that $k \to \infty$ implies*

$$\frac{L_n(f_{n+1}^{(m_k)})}{L_{n+1}(f_{n+1}^{(m_k)})} \to \infty.$$

Proof. For each n we prove by induction on k that for every $k \in N \cup \{0\}$ there is $m_k \in N$ such that

$$L_n(f_{n+1}^{(m_k)}) > k(n+1)^{m_k}.$$

From this and from the equality $L_{n+1}(f_{n+1}^{(m)}) = (n+1)^m$, which is valid for all $m \geqslant 0$, Theorem 1 follows:

For $k = 0$ it suffices to take $m_0 = 1$.

Let $k \geqslant 1$. By the induction hypothesis,

$$L_n(f_{n+1}^{(m_{k-1})}) > (k-1)(n+1)^{m_{k-1}}. \tag{9}$$

We set $p = (n+1)^{m_{k-1}}$. Then $p \geqslant 2$ and $1/m(p/(p-1))^{m/2} \to \infty$ as $m \to \infty$. Therefore, there exists an $m \in N$ such that

$$\frac{1}{m}\left(\frac{p}{p-1}\right)^{m/2} \geqslant 20k^4n^3m_{k-1}. \tag{10}$$

We set $m_k = mm_{k-1}$, $R = (p(p-1))^{m/2}$, and $r = (p/(p-1))^{m/2}$. Note that $Rr = p^m$ and $R/r = (p-1)^m$. With this notation, (10) becomes

$$r \geqslant 20k^4n^3m_k. \tag{11}$$

Let us prove an auxiliary statement.

Statement 1. *If g is a subfunction of the function $f_{n+1}^{(m_k)}$, then*

$$L_n(g) > \left(k + \frac{1}{r}\right) nes(g) - R.$$

Proof. We prove this by induction on $nes(g)$.

Let $nes(g) = 0$. Then from $R > 0$ it follows that $L_n(g) \geqslant 0 > 0 - R$.

Let $nes(g)\geqslant 1$, and let F be a formula in the basis $P_2(n)$ which computes the function g with complexity $L(F)=L_n(g)$. By (9), we can apply Lemma 4 to functions $f=f_{n+1}^{(m_{k-1})}$, to g as a subfunction of the function $f^{(m)}=f_{n+1}^{(m_k)}$, and to the number $q=k-1$. We thus obtain

$$N(k-1,F)\leqslant(nes(f_{n+1}^{(m_{k-1})})-1)^m=(p-1)^m. \tag{12}$$

Two cases are possible: (1) $nes(g)<p^m-kR$; (2) $nes(g)\geqslant p^m-kR$.

Case 1. The number of variables occurring in F at least k times is equal to $nes(g)-N(k-1,F)$. Therefore, $L(F)\geqslant k(nes(g)-N(k-1,F))$. From this, from (12), from the statement of Case 1, and from properties of R and r we have

$$\begin{aligned}L_n(g)=L(F)&\geqslant k(nes(g)-(p-1)^m)=k\cdot nes(g)-k\frac{R}{r}+R-R\\&=k\cdot nes(g)+\frac{1}{r}(p^m-kR)-R>\left(k+\frac{1}{r}\right)nes(g)-R.\end{aligned}$$

Case 2. We now introduce an auxiliary definition. Let G be an arbitrary μ-subformula of the formula F, and let $G_1,\ldots,G_s$ be all its immediate subformulas which compute linear functions. The formula G will be called *distinguished* if

all variables of $G_1,\ldots,G_s$ are nonsingular for the function g; (13)

the number of occurrences of each variable from $G_1,\ldots,G_s$ in F is equal to k; (14)

the total number of different variables in $G_1,\ldots,G_s$ is at most r. (15)

Assume that there exists a constants substitution A such that

$$nes(g)=nes(g|_A)+|A|; \tag{16}$$

$$L(F)\geqslant L(F|_A)+k|A|+1; \tag{17}$$

$$|A|\leqslant r. \tag{18}$$

Then from (17) it follows that $A\neq\emptyset$, i.e., $nes(g|_A)<nes(g)$. Therefore, we can apply the induction hypothesis to the function $g|_A$. Using (16)–(18), we obtain

$$\begin{aligned}L_n(g)=L(F)&\geqslant L(F|_A)+k|A|+1\geqslant L_n(g|_A)+k|A|+\frac{|A|}{r}\\&>\left(k+\frac{1}{r}\right)nes(g|_A)-R+\left(k+\frac{1}{r}\right)|A|=\left(k+\frac{1}{r}\right)nes(g)-R.\end{aligned}$$

Thus, under our assumption Statement 1 is proved.

Now we shall consider four cases which cover all possibilities:

(a) $m(F)>k$;

(b) the formula F has a distinguished fillable μ-subformula;

(c) the formula F has a distinguished center; and

(d) $m(F)\leqslant k$, all centers of the formula F are not distinguished and all distinguished subformulas of the formula F are non-fillable.

In cases (a)–(c) a constants substitution A satisfying conditions (16)–(18) will be produced, while in case (d) the statement will be proved independently.

Case (*a*). Let the number of occurrences of a variable x_i in F be at least $k+1$. By Lemma 6, there exists a constant c such that $nes(g)=nes(g|_{\{x_i=c\}})+1$. Let $A=\{x_i=c\}$. Then $|A|=1$, i.e., (16) is satisfied. The choice of the variable x_i implies (17), and from (11) it follows that $|A|=1\leqslant r$, i.e., (18) is satisfied.

Case (*b*). Let $G\equiv h(G_1,\ldots,G_s)$ be a distinguished and fillable μ-subformula of the formula F and, for definiteness, let G_1 be a distinguished subformula of the formula G which has a variable not present in $G_2,\ldots,G_s$. Let $\tilde{x}$ be the set of all variables occurring in formulas $G_2,\ldots,G_s$, and let $\Lambda_i(\tilde{x})$ for $i=2,\ldots,s$ be the function computed by the formula G_i. Since the subformula G_1 is distinguished, all functions Λ_i are linear.

Consider the function $\varphi(\tilde{x},y)=h(y,\Lambda_2(\tilde{x}),\ldots,\Lambda_s(\tilde{x}))$. If for any constants substitution $B=\{\tilde{x}=\tilde{c}\}$ the function $\varphi|_B$ essentially depends on y then $\varphi(\tilde{x},y)\equiv\varphi(\tilde{x},0)\oplus y$. Hence, the formula $h(0,G_2,\ldots,G_s)\oplus G_1$ computes the same function as the formula G, i.e., G has a linear representation, contrary to the property (r3) of reduced formulas. So, there exists a constants substitution $B_0=\{\tilde{x}=\tilde{c}_0\}$ such that $\varphi|_{B_0}$ does not depend on y.

Consider the system of linear equations

$$\Lambda_i(\tilde{x})=\Lambda_i(\tilde{}_0),\quad i=2,\ldots,s.$$

It is compatible, and the rank of the matrix of this system is not greater than the number of equations, which is $s-1$. Therefore, there exists a solution $\tilde{c}_1$ with at most $s-1$ coordinates equal to 1. Let $A=\{\tilde{x}=\tilde{c}_1\}$. From $\varphi(\tilde{c}_1,y)\equiv\varphi(\tilde{c}_0,y)$ it follows that $\varphi|_A$ does not depend on y, and then the formula $G|_A$ does not depend on subformula $G_1|_A$. Since the subformula $G_1|_A$ has a variable, which is not in $\tilde{x}$, the formula $F|_A$ after reduction will be simplified by at least one occurrence of variable. From this and (14) follows (17). The constants substitution A substitutes ones for at most $s-1\leqslant n-1=nes(f_{n+1})-2$ variables. Moreover, according to (13) all variables from $\tilde{x}$ are nonsingular for g. Using Lemma 7 we obtain (16). From (15) follows $|A|\leqslant r$, i.e., (18) is satisfied.

Case (*c*). Formula F has a distinguished center, which we shall denote by H. If each variable occurs in H at least once, then the formula H is fillable and we can employ the arguments of case (b). Let the variable x_i occur in H at least twice. Instead of A we shall choose a constants substitution defined on all variables from H except x_i and substituting for them the constant 0. Using (13), we apply Lemma 7 to get (16). Since the formula $H|_A$ depends only on x_i, after reduction it will have the complexity not exceeding 1. Thus, $F|_A$ is simplified by at least one occurrence of the variable x_i and according to (14) we have (17). From (15) follows (18).

Case (*d*). All centers of the formula F are not distinguished, all its distinguished subformulas are nonfillable, and $m(F)\leqslant k$. Suppose the proposition is not valid, i.e., $L_n(g)\leqslant(k+1/r)nes(g)-R$. Since the function g is the subfunction of the function

$f_{n+1}^{(m_k)}$, we have $nes(g) \leqslant (n+1)^{m_k} = p^m$. From this and from the equality $1/r = R/p^m$ we obtain

$$L(F) = L_n(g) \leqslant \left(k + \frac{1}{r}\right) nes(g) - R \leqslant \left(k + \frac{R}{p^m}\right) p^m - R = kp^m. \tag{19}$$

Statement (a) of Lemma 5 and the proposition of case 2 ($nes(g) \geqslant p^m - kR$) imply that

$$\begin{aligned} I(g) &\leqslant (nes(f_{n+1}) - 1)(nes(f_{n+1}^{(m_k)}) - nes(g)) \\ &= n(p^m - nes(g)) \leqslant nkR. \end{aligned} \tag{20}$$

By definition of the function f_{n+1}, $d(f_{n+1}) = nes(f_{n+1})$. Using the statement (b) of Lemma 5, the inequalities $nes(g) \geqslant p^m - kR$ and (20), the equality $Rr = p^m$, and (11), we obtain

$$\begin{aligned} d(g) &\geqslant nes(g) - I(g) \geqslant p^m - kR - nkR \geqslant rR - 2nkR \\ &\geqslant 20k^4n^3m_kR - 2nkR \geqslant 18k^4n^3m_kR. \end{aligned}$$

From this and from $R \geqslant 1$ it follows that $d(g) \geqslant 2$, i.e., the function g is nonlinear. Then by Lemma 1 we have

$$\mu(F) \geqslant \frac{1}{2n} d(g) + \frac{1}{2} \geqslant 9k^4n^2m_kR. \tag{21}$$

Let V be the number of not distinguished μ-subformulas of formula F, and let V_1, V_2, V_3 be the numbers of subformulas of the formula F not satisfying conditions (13), (14), and (15), respectively. Formulas which are immediate subformulas of different μ-subformulas of formula F and which compute linear functions are disjoint. Therefore, from $m(F) \leqslant k$ we obtain

$$V_1 \leqslant k \cdot I(g), \quad V_2 \leqslant (k-1) \cdot N(k-1, F), \quad V_3 \leqslant L(F)/r. \tag{22}$$

It follows from (12) that

$$N(k-1, F) \leqslant (p-1)^m \leqslant (\sqrt{p(p-1)})^m = R. \tag{23}$$

It follows from (19) and the equality $1/r = R/p^m$ that

$$L(F)/r = L(F) \cdot R/p^m \leqslant kp^mR/p^m = kR. \tag{24}$$

Adding up estimates (22), and taking into account (20), (23), and (24), we obtain

$$V \leqslant V_1 + V_2 + V_3 \leqslant k^2nR + (k-1)R + kR \leqslant 3k^2nR. \tag{25}$$

Let T be the maximum length of μ-chains of the formula F consisting only of distinguished μ-formulas. Since the number of distinguished μ-subformulas of the formula F is equal to $\mu(F) - V$, from Lemma 2 it follows that

$$T \cdot z(F) \geqslant \mu(F) - V.$$

Since the function g is nonlinear, $z(F) > 0$. From the condition of case (d) it follows that all centers of the formula F are not distinguished, which means that $V \geqslant z(F)$.

Thus, we have

$$\begin{aligned} T &\geqslant \frac{\mu(F)-V}{z(F)} \geqslant \frac{\mu(F)-V}{V} = \frac{\mu(F)}{V} - 1 \geqslant \quad \text{(see (21) and (25))} \\ &\geqslant \frac{9k^4n^2m_kR}{3k^2nR} - 1 = 3k^2nm_k - 1 \geqslant 2k^2nm_k \\ &\geqslant \text{(we use inequalities } k \geqslant \ln k + 1 \text{ and } n \geqslant \ln(n+1) \geqslant 1) \\ &\geqslant 2k(\ln k + 1)m_k \ln(n+1) = 2k(\ln k \ln(n+1)^{m_k} + \ln(n+1)^{m_k}) \\ &\geqslant (k+1)(\ln k + \ln(n+1)^{m_k}) = (k+1)\ln(kp^m). \end{aligned} \tag{26}$$

From the condition of case (d) it follows that all distinguished μ-subformulas of the formula F are nonfillable. Therefore, there is a μ-chain in F which has the length T and consists only of non-fillable μ-subformulas. Using Lemma 3, the condition $m(F) \leqslant k$, (26) and the inequality $(1+1/k)^{k+1} > e$, we obtain

$$L(F) \geqslant \left(1 + \frac{1}{m(F)}\right)^T \geqslant \left(1 + \frac{1}{k}\right)^{(k+1)\ln(kp^m)} > \mathrm{e}^{\ln(kp^m)} = kp^m.$$

This contradicts (19) and completes the proof of Statement 1.

Applying the statement proved above to the function $g = f_{n+1}^{(m_k)}$ and using the definition of p and equality $1/r = R/p^m$ we obtain

$$L_n(f_{n+1}^{(m_k)}) > \left(k + \frac{1}{r}\right)(n+1)^{m_k} - R = \left(k + \frac{R}{p^m}\right)p^m - R = k(n+1)^{m_k}. \qquad \square$$

Theorem 2. *$P_2(n+1) \prec P_2(n)$ for any $n \geqslant 2$.*

Proof. From inclusion $P_2(n+1) \supset P_2(n)$ it follows that $L_{n+1}(f) \leqslant L_n(f)$ for any f. Therefore, $P_2(n+1) \preccurlyeq P_2(n)$. From Theorem 1 it explicitly follows that the inverse inequality is not valid, i.e., by definition $P_2(n+1) \prec P_2(n)$. $\square$

Acknowledgements

The author is grateful to his supervisor O.B. Lupanov, N.A. Karpova, and M.I. Grinchuk for considerable help in preparing this paper.

References

[1] O.B. Lupanov, On complexity of realization of functions of algebra of logic by formulas, Problemy kibernetiki 3 (Moscow, Fizmatgiz, 1960) 61–80 (in Russian).
[2] B.A. Muchnik, Complexity bound for realization of linear function in some bases, Kibernetika 4 (1970) 29–38 (in Russian).
[3] V.A. Stetsenko, On almost bad bases in P_2, Matematicheskie voprosy kibernetiky 4 (Moscow, Nauka, 1992) 139–177 (in Russian).
[4] B.A. Subbotovskaya, On comparison of bases under realization of functions of Boolean algebra by formulas, Dokl. AN SSSR 149(4) (1963) 784–787 (in Russian).